Bravura Security

Global Manufacturer Reduces Audit Overhead and Scales Privileged Access Automation

CASE STUDY

CHALLENGE Audit overhead increased and visibility declined as an aging, heavily customized PAM platform caused inconsistent password rotation, limited visibility, and high audit overhead across a complex global manufacturing environment.
SOLUTION Bravura Privilege delivered automated discovery, rotation, brokering, and delegated management across tens of thousands of privileged accounts and systems worldwide.
OUTCOME Millions in annual efficiency gains with payback measured in weeks. The organization now maintains continuous privileged access automation, and clearer audit evidence.

Global CPG

GLOBAL CONSUMER PACKAGED GOODS COMPANY

INDUSTRY
Manufacturing

REGION
Worldwide

SOLUTIONS
Bravura Privilege

A top global consumer packaged goods (CPG) manufacturer operating hundreds of production plants and business sites worldwide needed a better way to control privileged access at scale. Their existing platform had become brittle, dependent on custom scripts, and unable to keep pace with growing security, audit, and operational demands. To build a stronger foundation for identity and privileged access security, the organization turned to Bravura Privilege.

CHALLENGE

As one of the world's largest CPG manufacturers, the organization operates a vast and diverse ecosystem: factories, distribution centers, R&D sites, global offices, hybrid-cloud infrastructure, and thousands of administrators who support business-critical operations.

Their previous privileged access solution was approaching end of life. Over years of growth, it had been patched together with local scripts and one-off utilities. Static vaulting was still widespread. Password rotation was ad hoc in many regions, especially across industrial systems that required precise coordination during patching windows.

Audits were increasingly difficult. Proving who had access to what and when meant combing through screenshots, exporting logs, and relying on tribal knowledge to explain exceptions. A small central IAM team carried the full burden of onboarding new platforms, managing exceptions, and answering audit questions. When the incumbent platform's retirement became inevitable, leaders knew they could not simply swap one tool for another. They needed:

- **Consistent, automated password rotation** across the global estate
- **Unified audit trail** for personal and shared privileged access
- **Delegated operations** so regions and platform owners could manage their own systems safely
- **A platform engineered for enterprise-scale automation**, not manual oversight

The search began for a long-term PAM partner that could support tens of thousands of privileged accounts, diverse infrastructure, and continuous automation.

SOLUTION

The organization launched a competitive evaluation that included a full RFP and hands-on proof of concept. Bravura Privilege stood out from the incumbent and other major industry vendors for several reasons.

1. **Broad, enterprise-ready connector ecosystem.** The platform demonstrated strong, built-in integrations for Active Directory, Azure AD, Linux, AIX, SAP, ESXi, Checkpoint, and specialized manufacturing systems.

2. **A more intuitive, unified experience.** Teams saw immediate improvements in how access requests, approvals, and privileged sessions flowed end to end.
3. **Distributed yet governed operations.** Bravura Privilege enabled safe delegation to platform teams and regional administrators while preserving central policy enforcement.
4. **A single license model.** Unlike other vendors that required multiple modules or added infrastructure, Bravura Privilege offered full PAM capability under a unified license.
5. **Real-world integration during the POC.** Instead of demonstrating abstract screens, Bravura wired the POC into the customer's identity sources, ticketing system, and a representative infrastructure set. This allowed the team to validate real workflows, not just features.
6. **Extensibility without code forking.** Custom business logic could be added through configuration and Python extensions, stored in Git, and deployed across dev, test, and production environments.

The migration occurred in controlled waves over ten months. Early waves replaced the legacy platform. Later waves expanded automation, especially around service accounts that supported industrial systems where timing and sequencing were critical.

OUTCOME

Today, the organization operates one of the most mature global PAM programs in its industry, centered on continuous privileged access automation.

Enterprise-Scale Coverage

Bravura Privilege manages:

- 14.5k+ personal admin accounts
- 51k+ shared privileged accounts
- 34k+ actively connecting systems

Continuous Automation

On schedule, the platform executes:

- 200k automated password rotations monthly
- 150k+ audited password checkouts every month
- 320k+ secure disclosure events every 90 days

Password randomization compliance remains at 97 to 99%, even across complex manufacturing environments.

Audit-Ready Evidence

Auditors can now validate exactly:

- Who accessed which privileged credential
- When it was used
- Which approvals were granted
- Whether policies were followed

The organization saves an estimated 2,700 audit-related hours per year, eliminating manual evidence collection and reducing exceptions.

Major Financial Impact

Using jointly validated ROI modeling, the organization estimates:

- $4M in annual operational efficiency gains
- $1M in annualized credential-abuse risk reduction
- Payback measured in weeks
- Annual program cost in the low-to-mid six figures

"Bravura Security stood out by building an extensive POC tailored to our requirements and went the extra mile to make sure the solution being proposed would fulfil our requirements."

SENIOR LEADER
Global Consumer Packaged Goods Co.

NEXT STEPS

The organization continues to expand the program with:

- Broader PAM coverage across public cloud
- More stringent end-to-end session brokering
- Improved SAP connector refinement
- Enhanced analytics for risk and audit teams
- Greater delegation for onboarding while centralizing governance

The program now operates on predictable 1–2-month sprints, with most enhancements driven by internal teams and supported by Bravura Security as needed.

Bravura Security
bravurasecurity.com
sales@bravurasecurity.com